PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G11B 3/90, 23/28, 3/64, H04L 9/00

A1

(11) International Publication Number: **WO 98/29869**

(43) International Publication Date: 9 July 1998 (09.07.98)

(21) International Application Number: PCT/US97/23441

(22) International Filing Date: 17 December 1997 (17.12.97)

(30) Priority Data:
08/768,219 17 December 1996 (17.12.96) US

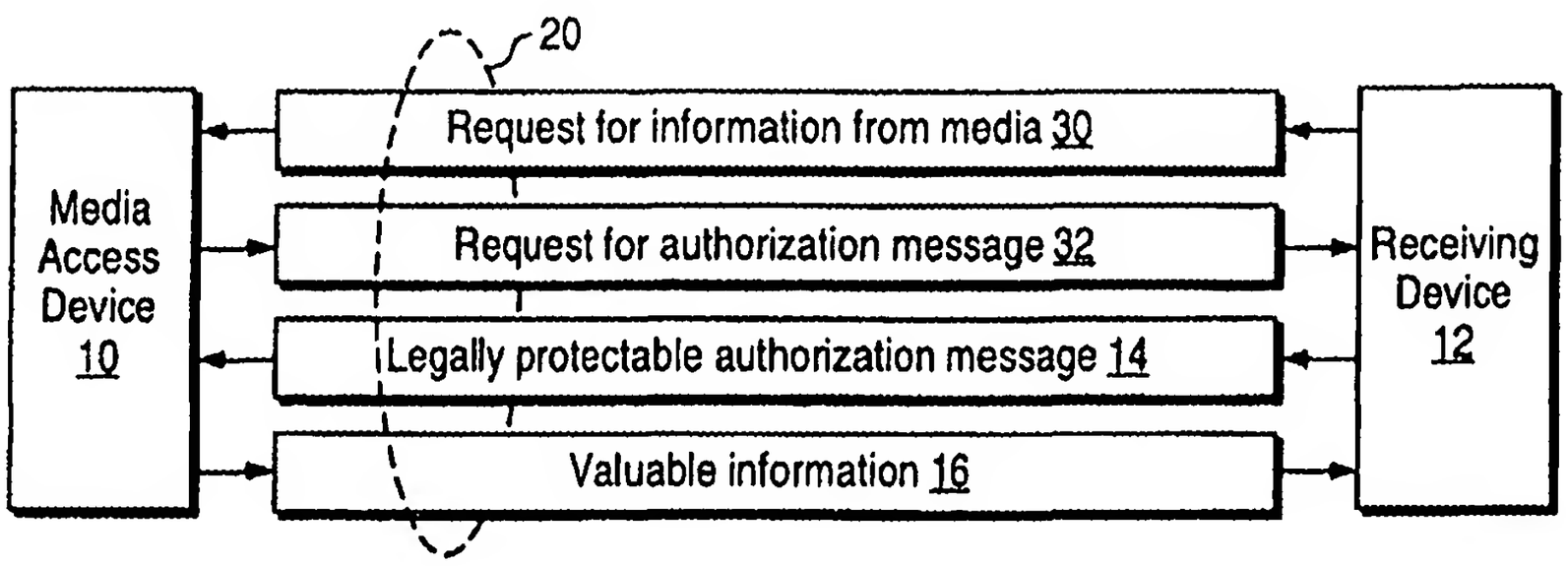
(71)(72) Applicant and Inventor: LESKE, Lawrence, A. [US/US]; 724 Knoll Drive, San Carlos, CA 94070 (US).

(74) Agent: HORSTMANN, Paul, H.; 2100 Northpoint #102, San Francisco, CA 94123 (US).

(81) Designated States: BR, CA, JP, KR, MX, Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ACCESS TO INFORMATION USING PROTECTABLE AUTHORIZATION MESSAGES



(57) Abstract

A system for preventing unauthorized use of valuable information (16) using a predetermined authorization message (14) which is protectable under intellectual property laws. The system includes a media access device (10) that enables access to the valuable information (16) which provides the valuable information (16) to a receiving device (12) in the system only if the receiving device (12) produces the predetermined authorization message (14).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

ACCESS TO INFORMATION USING PROTECTABLE AUTHORIZATION MESSAGES

Technical Field

The present invention pertains to the field of accessing valuable information. More particularly, this invention relates to a method for accessing valuable information using legally protectable authorization messages.

Background Art

Valuable information such as movies, videos, and audio recordings is commonly distributed to consumers using a variety of distribution media including magnetic storage media and optical storage media. Such magnetic storage media includes magnetic tape and magnetic disk media. Such optical storage media includes compact disks, laser disks, minidisks, as well as digital video disks and writeable optical storage disks.

Content providers of such valuable information usually seek to prevent unauthorized use the valuable information distributed on such media. Typically, unauthorized use of such valuable information may be prohibited under the intellectual property protection laws of the United States and other countries. An owner of the intellectual property rights to the valuable information is referred to as a right holder.

For example, unauthorized copying of the valuable information contained on such media may be prohibited under United States and international copyright laws. Movies, videos, and other content distributed on media such as video tape, laser disk and digital video disk are usually protected from unauthorized copying under copyright laws. The right holder of such valuable information nevertheless is faced

with the prospect of preventing violations of their intellectual property rights.

Typically, the prevention of intellectual property right violations is facilitated through formal agreements between the right holders and the manufactures of media recording/playback devices. Under one such prior agreement, a copyright indication is contained on storage media that holds valuable information which is prohibited from being copied. Typically, the manufacturers of authorized media recording/playback devices disable recording functions if the copyright indication is detected while reading the media.

These efforts notwithstanding, third parties often provide devices capable of defeating such agreed safeguards against copying of valuable information. For example, such devices may filter or eliminated the copyright indication as the content of the storage media is read and transferred to a recording device. Typically, right holders seek to cut off the source of such devices to prevent copying of their valuable information.

One way to cut off the source of such devices is to bring legal actions against the providers of such devices for copyright violation. However, a defense to such an action is to argue that such devices are provided for uses other than copying of valuable information. Unfortunately, such a defense may hinder the efforts of right holders seeking to enforce their rights and cut off the supply of such devices.

DISCLOSURE OF THE INVENTION

A system and method is disclosed for preventing unauthorized use of valuable information using legally protectable authorization messages. A media access device that enables access to the valuable information provides the valuable information to a receiving device only if the receiving device produces the legally protectable authorization message. The legally protectable authorization message may be prohibited from unauthorized use under international intellectual property laws of the United States and other countries.

Accordingly, providers of unauthorized devices violate an intellectual property rights in the legally protected authorization message if those devices produce the legally protectable authorization message. For example, an unauthorized device must generate a copyrighted authorization message in order to obtain the valuable information from the media. As a consequence, right holders can more easily show that providers of such unauthorized devices are providing the devices in order to wrongly obtain valuable information from storage media.

Other features and advantages of the present invention will be apparent from the detailed description that follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is described with respect to particular exemplary embodiments thereof and reference is accordingly made to the drawings in which:

Figure 1 illustrates a method for preventing unauthorized use of valuable information which is accessed by a media access device;

Figure 2 illustrates a method for preventing unauthorized use of the valuable information in another embodiment;

Figure 3 illustrates a method for preventing unauthorized use of the valuable information in yet another embodiment;

Figure 4 illustrates a system that employs legally protectable authorization messages to prevent unauthorized use of valuable information;

Figure 5 illustrates a media access device in one embodiment;

Figure 6 illustrates a process by which a media access device prevents unauthorized used of valuable information by devices coupled to a communication path.

MODES FOR CARRYING OUT THE INVENTION

Figure 1 illustrates a method for preventing unauthorized use of valuable information 16 which is accessed by a media access device 10. A receiving device 12 transfers a legally protectable authorization message 14 to the media access device 10 via a communication path 20. The media access device 10 receives the legally protectable authorization message 14 and then transfers the valuable information 16 to the receiving device 12 via the communication path 20 if the legally protectable authorization message 14 is provided and is validated by the media access device 10.

Unauthorized use of the legally protectable authorization message 14 may be prohibited under intellectual property laws. If the receiving device 12 is provided by an entity not authorized to use the legally protectable authorization message 14 by the right holder to the legally protectable authorization message 14 then that entity may be liable for violating the intellectual property rights afforded to the right holder regardless of the intended or actual use of the receiving device 12.

In some embodiments, the legally protectable authorization message 14 is a predefined copyrighted message. The predefined copyrighted message includes a copyright notice that specifies the owner of the copyright. In one embodiment, the legally protectable authorization message 14 is an ASCII coded message. In another embodiment, the legally protectable authorization message 14 is an encrypted message.

In some embodiments, the legally protectable authorization message 14 includes a predefined encryption key which is used to decode the valuable information 16. The predefined encryption key is kept secret by the right holder to the legally protectable authorization message 14 and is disclosed only to approved device providers that adhere to the present methods for accessing valuable information. In one embodiment, the predefined encryption key contained in the legally protectable authorization message 14 is ASCII encoded. In another embodiment, the predefined encryption key contained in the legally protectable authorization message 14 is an algorithmic transformation of the actual key such as the actual key minus one.

The media access device 10 represents a wide variety of devices capable of accessing valuable information including media players such as digital video disk or DVD players, laser disk players, compact disk players, CD-ROM players, video tape players, and audio tape players. The media access device 10 also represents computer systems including personal computer systems which are capable of reading information from a variety of media including DVD media, CD-ROM media, as well as other magnetic and optical storage media.

The receiving device 12 represents a wide variety of devices capable of using the valuable information 16 including media recorders such as digital video recorders, video tape recorders, and audio tape recorders. The receiving device 12 also represents devices capable of rendering the valuable information 16 included display devices such as display monitors, video monitors, and television monitors any of which may have audio rendering capabilities. The receiving device 12 also represents computer systems including personal computer systems which

are capable of recording the valuable information 16 or for manipulating the valuable information 16 or for rendering the valuable information 16 via a variety of display mechanisms.

The receiving device 12 also represents devices which are not authorized by the right holder of the message 14 to use the message 14. Such devices may be embodied as any of the devices listed above or specialized devices that are placed between a media access device and another unauthorized receiving device such as any of the receiving devices listed above.

The communication path 20 represents any communication path capable of carrying the legally protectable authorization message 14 and the valuable information 16. The communication path may be embodied in a parallel communication bus structure, a serial communication bus structure, a parallel or serial communication link, a communication network, or an infrared or radio frequency communication link or communication network. The communication path 20 may be a standardized communication path that is provided specifically for carrying the legally protectable authorization message 14 and the valuable information 16 and for enabling access to protected information by authorized devices.

The valuable information 16 may be subdivided into a series of information blocks with each block being encrypted using various encryption methods. Block transformation encryption methods may be used to sufficiently manipulate the content of the valuable information being transferred to prevent viewing or listening without appropriate decryption. The content of the valuable information 16 may also be encoded according to various compression techniques including

MPEG, International Standards Organization SC29WG11, approved compression standards and FCC approved compression standards.

Figure 2 illustrates another method for preventing unauthorized use of the valuable information 16 which is accessed by the media access device 10. The media access device 10 transmits a poll message 22 to the receiving device 12 via the communication path 20. The poll message 22 includes a request authorization message. The receiving device 12 responds to the poll message 22 containing the request authorization message by transferring a response message 24 via the communication path 20 that contains the legally protectable authorization message 14. Any one of a wide variety of known poll/response communication techniques may be used by the media access device 10 to poll the receiving device 12 and other devices coupled to the communication path 20.

The media access device 10 receives the legally protectable authorization message 14 contained in the response message 24 and then logs the receiving device 12 as an authorized receiving device if the legally protectable authorization message 14 is valid. The media access device 10 may transmit the poll message 22 to the receiving device 12 at power up or whenever a media element is inserted into the media access device 10 or whenever the receiving device 12 is first detected on the communication path 12.

At any time, the receiving device 12 transfers a request for information from media message 30 to the media access device 10 via the communication path 20. If the media element in the media access device 10 contains valuable information which may not be used without authorization and

if the receiving device 12 is logged as an authorized receiving device then the media access device 10 responds to the request 30 by transferring the valuable information 16 obtained from the media element via the communication path 20. If the media element in the media access device 10 contains information which may not be used without authorization and if the receiving device 12 is not logged as an authorized receiving device then the media access device 10 either ignores the request 30 or transfers a request denied message to the receiving device 12 via the communication path 20. In one embodiment, the media access device 10 determines whether the media element contains valuable information which may not be used without authorization by reading the media element for an indication of whether the information contained thereon may be used without authorization.

Figure 3 illustrates yet another method for preventing unauthorized use of the valuable information 16 which is accessed by the media access device 10. The receiving device 12 transfers the request message 30 to the media access device 10 via the communication path 20. If the media element in the media access device 10 contains valuable information which may not be used without authorization then the media access device 10 transfers a request authorization message 32 to the receiving device 12 via the communication path 20.

If the receiving device 12 responds to the request message 32 with the legally protectable authorization message 14 then the media access device 10 transfers the valuable information 16 via the communication path 20. If the receiving device 12 does not produce the legally protectable authorization message 14 in response to the request message

32 then the media access device 10 either ignores the request message 30 or transfers a request denied message to the receiving device 12 via the communication path 20.

Figure 4 illustrates a system 50 that employs legally protectable authorization messages to prevent unauthorized use of valuable information. The system 50 includes the media access device 10, a television system 40, a recording system 42, a computer system 44, and a pair of unauthorized receiving devices 46 and 48 all coupled to the communication path 20. Any one or more of the television system 40, the recording system 42, the computer system 44, and the unauthorized receiving devices 46 and 48 may provide the functionality of the receiving device 12 with respect to obtaining valuable information from media being accessed by the media access device 10.

The unauthorized receiving device 46 represents a device that does not produce the legally protectable authorization message 14 when required. The unauthorized receiving device 48 represents a device that does produce the legally protectable authorization message 14 but that is provided by an entity that is not authorized to use the legally protectable authorization message 14 by the owner of the intellectual property rights in the legally protectable authorization message 14. For example, the unauthorized receiving device 48 may be manufactured by an entity not licenced by the owner of the copyright on the legally protectable authorization message 14.

In one embodiment, the media access device 10 sends polling messages to each of the devices 40-48 at power up time or at the time a new media element containing valuable information which may not be used without authorization is

placed into the media access device. The media access device 10 maintains a log of which of the device 40-48 returned the legally protectable authorization message 14 in response to the polling messages. Thereafter, the media access device 10 uses the information in the log to either satisfy or deny any requests for valuable information received from the devices 40-48.

Figure 5 illustrates the media access device 10 in one embodiment. The media access device 10 includes a media access mechanism 60 for reading information from a storage media. The information on the storage media may be valuable information which is protected by copyright laws and which may not be used without authorization. The media access device 10 includes a communication interface 64 which enables transfer of information over the communication path 20 including the valuable information 16 obtained from the storage media and messages used to obtain authorization from the devices 40-48.

The media access device 10 includes a processor 62 that generates messages and that maintains a log of authorized devices in a memory 66. The processor 62 and the memory 66 may in some embodiments be the same processor and memory elements in the media access device 10 which are used to access the storage media.

Figure 6 illustrates a process by which the media access device 10 prevents unauthorized used of valuable information by devices coupled to the communication path 20. At block 100, the processor 62 transfers poll messages to each of the devices 40-48 via the communication path 20. The processor 62 may poll each device individually or may broadcast one poll to all devices via the communication path 20.

At block 102, the processor 62 creates a log of authorized receiving devices. A logged authorized receiving device is a receiving device on the communication path 20 that returned the legally protectable authorization message 14 in response to a poll. This log may be stored in the memory 66.

At block 104, an information request is received from one of the devices 40-48 via the communication path 20. At block 106, the processor 62 determines whether the information request received at block 104 is a request for valuable information which may not be used without authorization. In one embodiment, the media being accessed through the media access mechanism 60 stores an indication of whether the media contains valuable, i.e. copyrighted, information which may not be used without authorization.

If the requested information is not valuable information requiring authorization then at block 108 the processor 62 transfers the requested information to the requesting receiving device via the communication path 20 without regard as to whether the requesting receiving device is an authorized device. Otherwise, control proceeds to block 110.

At block 110, the processor 62 determines whether the requesting receiving device is an authorized receiving device by accessing the log of authorized receiving devices contained in the memory 66. If the requesting receiving device is authorized then the processor 62 transfers the valuable information to the requesting receiving device at block 112. Otherwise, the processor 62 ignores the information request and proceeds back to block 104 to handle a next information request.

In an alternative embodiment, the processor 62 ignores the information request at block 110 if any one or more of the devices 40-48 is unauthorized. This embodiment prevents unauthorized receiving devices from eavesdropping on transactions conducted by other authorized devices coupled to the communication path 20.

The foregoing detailed description of the present invention is provided for the purposes of illustration and is not intended to be exhaustive or to limit the invention to the precise embodiment disclosed. Accordingly, the scope of the present invention is defined by the appended claims.

CLAIMS

What is claimed is:

1. A system for preventing unauthorized use of valuable information, comprising:

receiving device that generates a legally protectable authorization message;

media access device that transfers the valuable information to the receiving device in response to the legally protectable authorization message.

2. The system of claim 1, wherein the legally protectable authorization message includes a copyright notice.

3. The system of claim 2, wherein the copyright notice identifies a right holder of the legally protectable authorization message.

4. The system of claim 1, wherein the receiving device and the media access device are coupled to a communication path that carries the legally protectable authorization message and the valuable information.

5. The system of claim 1, wherein the valuable information is contained on a storage media which is read by the media access device.

6. The system of claim 5, wherein the storage media contains an indication that the valuable information may not be used without authorization.

7. The system of claim 6, wherein the media access device does not transfer the valuable information to the receiving

device if the indication is present on the storage media unless the receiving device provides the legally protectable authorization message.

8. The system of claim 6, wherein the media access device transfers the valuable information to the receiving device if the indication is not present on the storage media regardless of whether the receiving device provides the legally protectable authorization message.

9. A system for preventing unauthorized use of valuable information, comprising:

means for reading the valuable information from a storage media;

means for obtaining a legally protectable authorization message from each of a plurality of receiving devices;

means for transferring the valuable information to a requesting one of the receiving devices if the requesting one provides the legally protectable authorization message.

10. The system of claim 9, wherein the means for obtaining comprises:

means for polling each of the receiving devices;

means for logging the receiving devices that produce the legally protectable authorization message.

11. The system of claim 10, wherein the means for reading comprises a media player for reading the storage media.

12. The system of claim 11, wherein the means for polling comprises means for polling the receiving devices in response to the placement of the storage media into the media player.

13. The system of claim 11, wherein the means for polling comprises means for polling the receiving devices in response to the placement of the storage media into the media player if the storage media indicates that the valuable information may not be used without authorization.

14. The system of claim 10, wherein the means for transferring the valuable information comprises means for transferring the valuable information to the requesting one of the receiving devices if the requesting one is logged as one of the receiving devices that produce the legally protectable authorization message.

15. The system of claim 10, wherein the means for transferring the valuable information comprises means for transferring the valuable information to the requesting one of the receiving devices only if all of the receiving devices are logged as receiving devices that produce the legally protectable authorization message.

16. A method for preventing unauthorized use of valuable information, comprising the steps of:

reading the valuable information from a storage media;

obtaining a legally protectable authorization message from each of a plurality of receiving devices;

transferring the valuable information to a requesting one of the receiving devices if the requesting one provides the legally protectable authorization message.

17. The method of claim 16, wherein the step of obtaining comprises the steps of:

polling each of the receiving devices;

logging the receiving devices that produce the legally protectable authorization message.

18. The method of claim 17, wherein the step of transferring the valuable information comprises the step of transferring the valuable information to the requesting one of the receiving devices if the requesting one is logged as one of the receiving devices that produce the legally protectable authorization message.

19. The method of claim 17, wherein the step of transferring the valuable information comprises the step of transferring the valuable information to the requesting one of the receiving devices only if all of the receiving devices are logged as receiving devices that produce the legally protectable authorization message.

FIG. 1

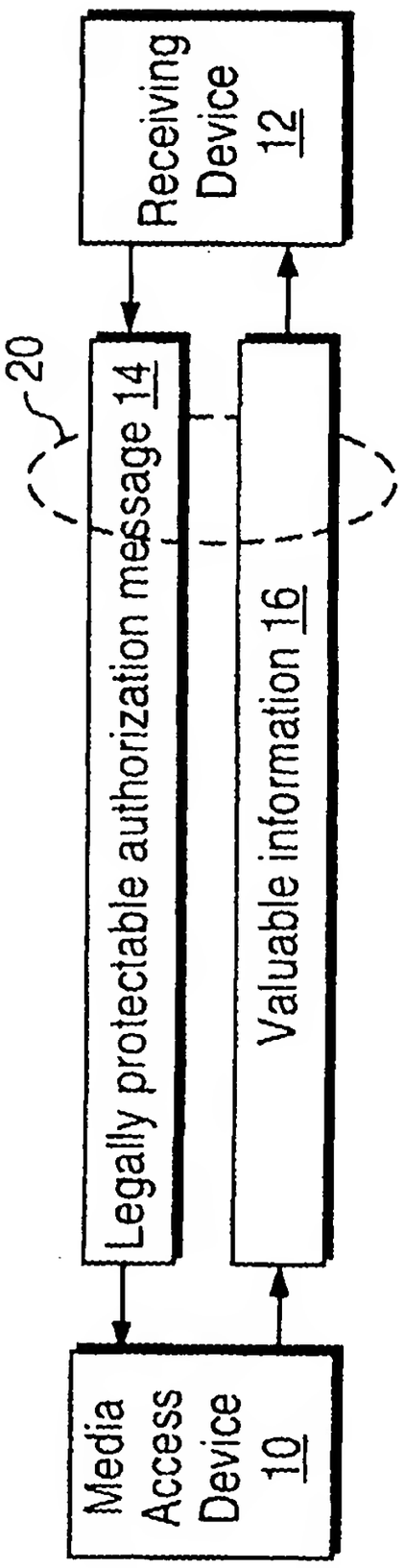
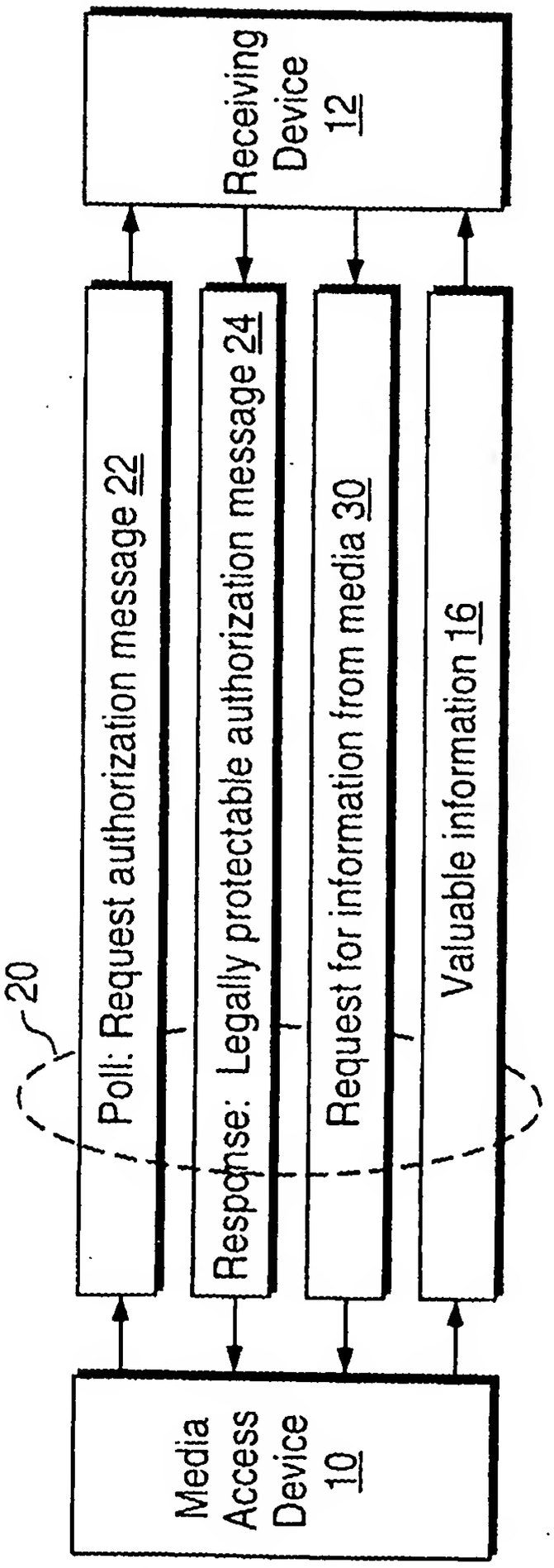

Receiving Device 12
20
Legally protectable authorization message 14
Valuable information 16
Media Access Device 10

FIG. 2


Receiving Device 12
20
Poll: Request authorization message 22
Response: Legally protectable authorization message 24
Request for information from media 30
Valuable information 16
Media Access Device 10

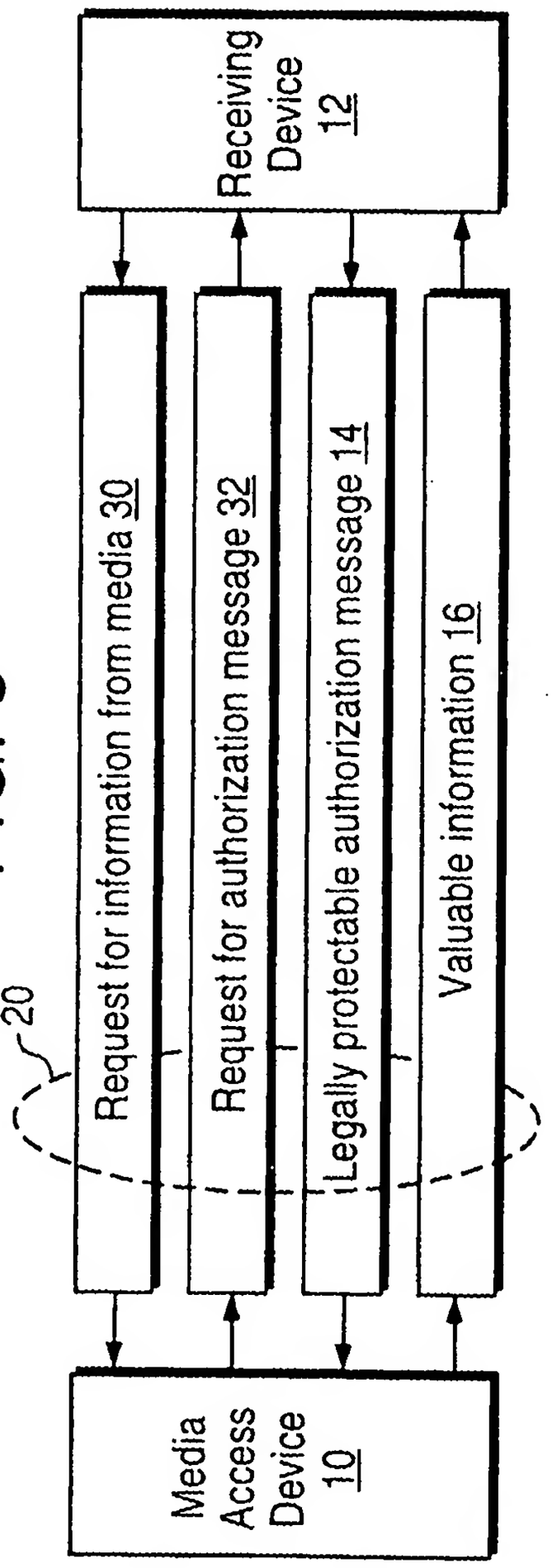

Receiving Device 12
Request for information from media 30
Request for authorization message 32
Legally protectable authorization message 14
Valuable information 16
20
Media Access Device 10

FIG. 3

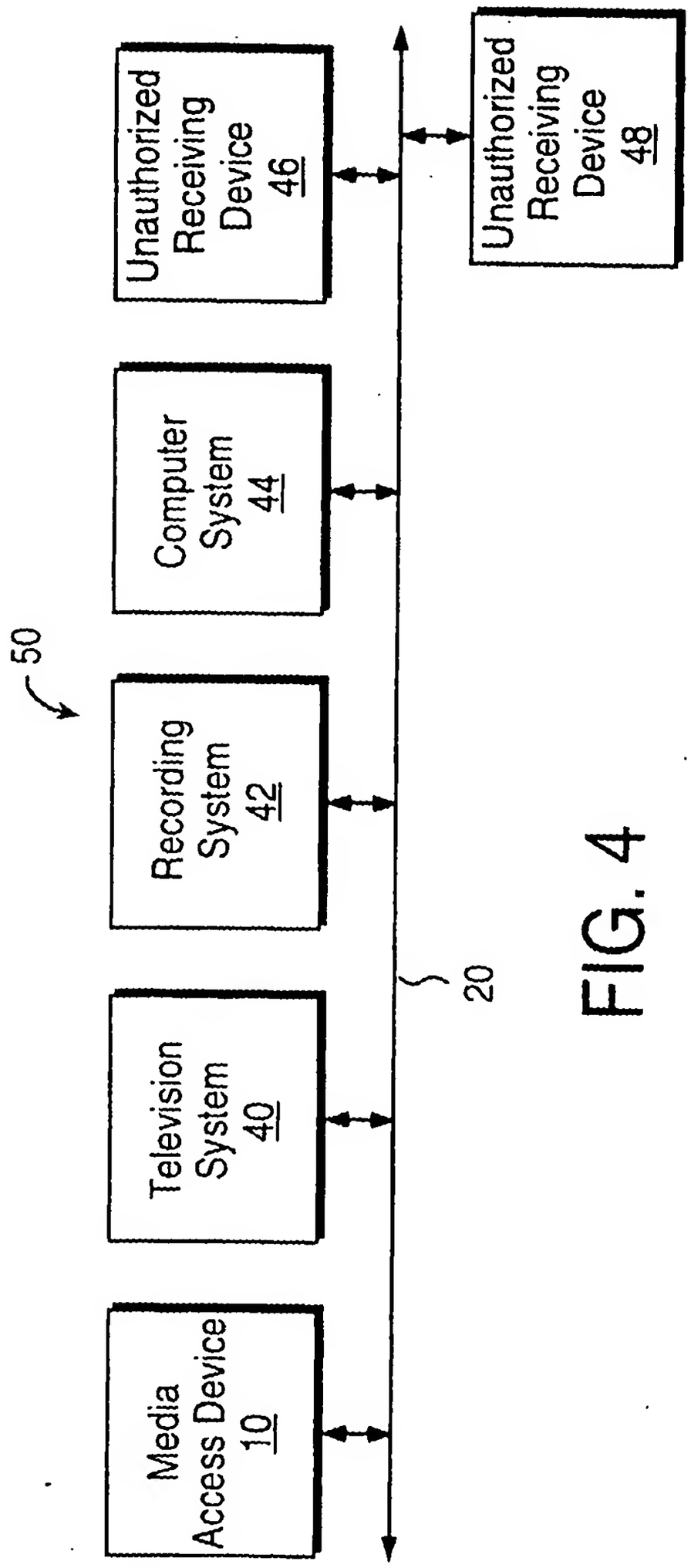
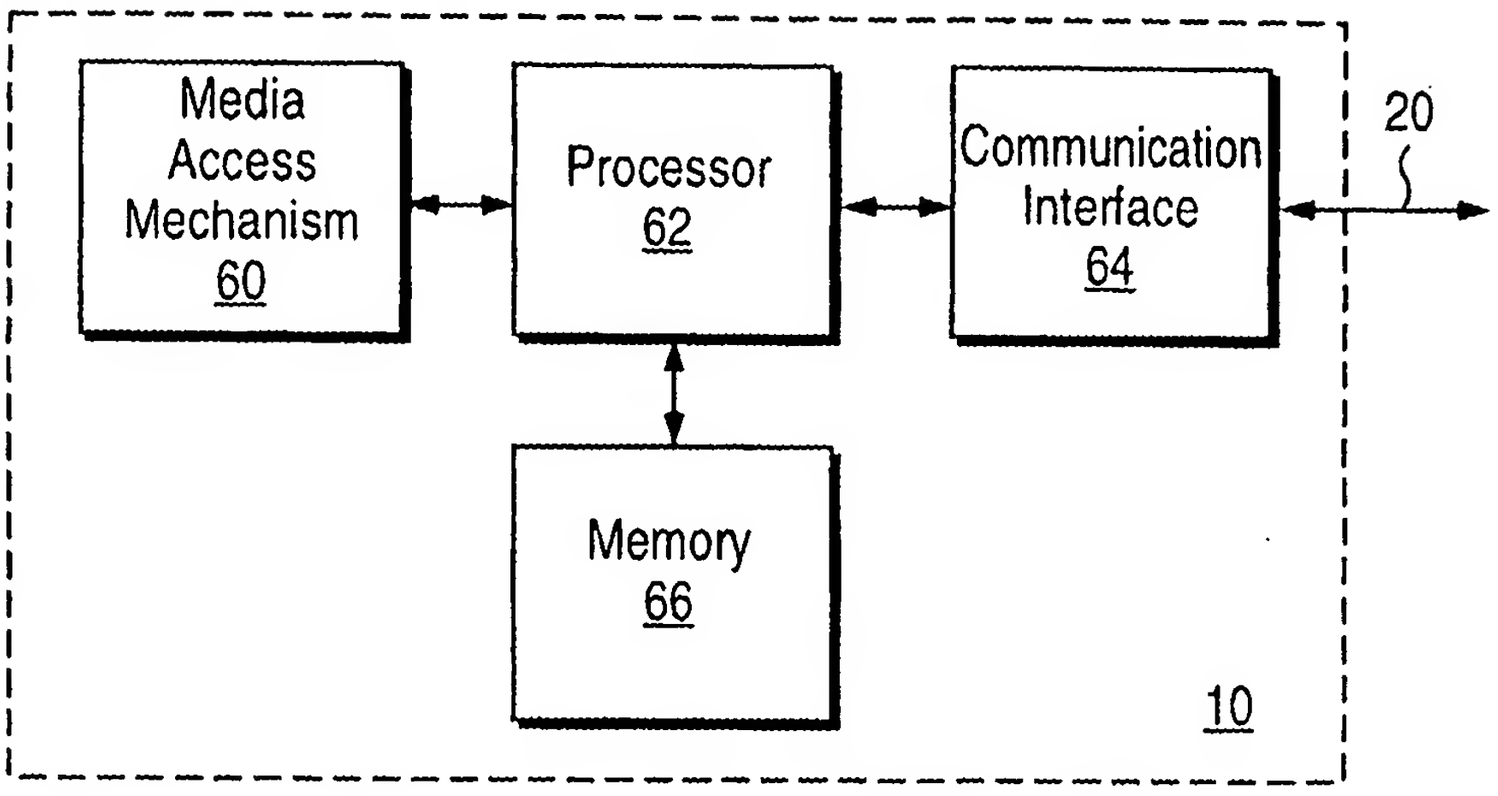

Unauthorized Receiving Device 46
Unauthorized Receiving Device 48
Computer System 44
Recording System 42
Television System 40
50
20
Media Access Device 10

FIG. 4

FIG. 5


Media Access Mechanism 60
Processor 62
Communication Interface 64
20
Memory 66
10

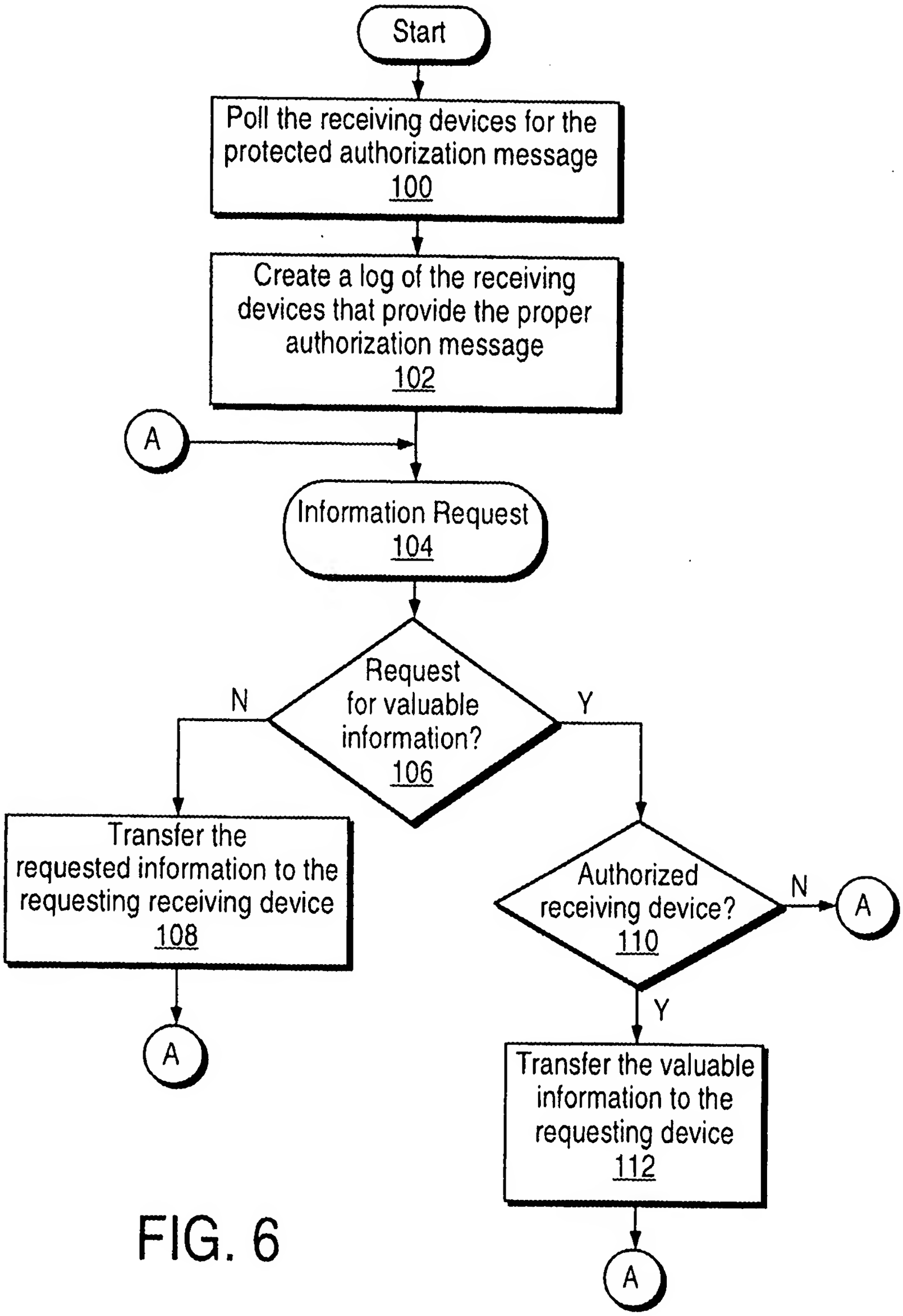

Start
Poll the receiving devices for the protected authorization message 100
Create a log of the receiving devices that provide the proper authorization message 102
A
Information Request 104
Request for valuable information? 106
N
Y
Transfer the requested information to the requesting receiving device 108
A
Authorized receiving device? 110
N
A
Y
Transfer the valuable information to the requesting device 112
A

FIG. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23441

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G11B 3/90, 23/28, 3/64; H04L 9/00
US CL : 369/32, 58, 47, 84; 380/3, 4, 9, 21, 25, 49, 66

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 369/32, 58, 47, 84; 380/3, 4, 9, 21, 25, 49, 66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS
searched terms:encryption(4a)key(P)(prevent? or illegal or unauthorized)(p)(disk or disc or medium)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,412,718 A (NARASIMHALU et al) 02 May 1995, cols. 5 and 6, and fig 6A.	1-19
Y	US 5,416,840 A (CANE et al) 16 May 1995, col.4 line 49 to col. 6 line 44.	1-19
Y,P	US 5,651,064 A (NEWELL) 22 July 1997, col. 3,l ine 1 to col. 5 line 60.	1-19
Y,E	US 5,715,403 A (STEFIK) 03 February 1998, figs 1-3.	1-19
Y	US 5,453,968 A (VELDHUIS et al) 26 September 1995, fig 7.	1-19
Y,P	US 5,661,703 A (MORIBE et al) 26 August 1997, col.13, line 49 to col. 16, line 39.	1-19

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 APRIL 1998	10 JUN 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-9051	Authorized officer NABIL HINDI Telephone No. (703) 308-1555

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/23441

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,570,339 A (NAGANO) 29 October 1996, figs 7-12.	1-19